AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States Courts
Southern District of Texas
FILED
April 04, 2023
Nathan Ochsner, Clerk of Court

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

SAMSUNG CELLULAR TELEPHONE
IMEI: 357299882022186

Case No. **4:23-mj-651**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

(See Attachment A)

located in the Southern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

(See Attachment B)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1344	Bank Fraud
18 USC 1028A	Aggravated Identity Theft

The application is based on these facts:
See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jacqueline Olivas, Special Agent
Printed name and title

Submitted by reliable electronic means, sworn to, signature attested telephonically per Fed.R.Crim.P. 4.1, and probable cause found

Date: 04/04/2023

Judge's signature

City and state: Houston, TX

Sam S. Sheldon , U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF SAMSUNG CELLULAR TELEPHONE IMEI: 357299882022186 CURRENTLY LOCATED AT 25700 I-45 NORTH SUITE 200, HOUSTON, TEXAS.	Case No. **4:23-mj-651**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Jacqueline Olivas, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I, Jacqueline Olivas, am assigned as a Special Agent (SA) with the Department of Homeland Security (DHS) with Homeland Security Investigations (HSI), Immigration and Customs Enforcement (ICE). I am currently assigned to the HSI office in Houston, Texas. I am empowered by the DHS as a SA to execute arrests, searches, and seizures for violations of Titles 8, 18, 19, 21, and 31 of the United States Code and related offenses. I have been a SA for HSI since March of 2019. Previously, I was an Asylum Officer from May of 2018 to March of 2019 employed by the United States Citizenship and Immigration Services (USCIS). Before that, I was a Customs and Border Protection Officer (CBPO) from February of 2016 to May of 2018. I

attended the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia for my CBPO Basic Law Enforcement Training, Asylum Adjudications Training, and Criminal Investigator Training.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a black Samsung cellular telephone, IMEI: 357299882022186, hereinafter the "DEVICE," recovered from Kevin Daniel BISHOP at the time of his arrest on January 22, 2023. The DEVICE is currently located at 25700 I-45 North Suite 200, Houston, Texas.

5. The applied-for warrant would authorize the forensic examination of the DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

1. In January of 2023, Department of Public Safety (DPS), Texas Highway Patrol notified the HSI Houston, Texas Document Benefit Task Force (DBFTF) that they arrested Kevin Daniel BISHOP (BISHOP) on December 15, 2022, in Houston, Texas, for Tamper with Government Documents and Fraud Use/Possession of Identifying Information. At the time, BISHOP was encountered with two counterfeit U.S. passport cards which contained his photograph and real persons identifying information (name, date of birth, etc.). DPS informed the HSI DBFTF that BISHOP had an extensive criminal history, including fraud related charges. DPS also advised that they had received information from the Montgomery County Sheriff's Office

(MCSO) and the Baytown Police Department (BPD) linking BISHOP to several bank fraud incidents in the Houston area.

2. The HSI DBFTF followed up with the detectives from MCSO and BPD and the financial institutions affected. A review of the information revealed that BISHOP had been to different branches of three financial institutions in the Houston area to commit bank fraud. BISHOP utilized counterfeit documents, including U.S. passport cards, to impersonate bank customers and complete fraudulent withdrawals.

3. Furthermore, a cellphone data extraction report, as a result of a search warrant for BISHOP's Android OnePlus cellular telephone seized on December 15, 2022 (BISHOP's arrest), contained photographs of counterfeit documents and victims' personal identifiable information (PII). The extraction report also had messages containing victims' PII and information on tellers available and lines (at the bank). A review of the video surveillance collected from multiple banks shows that BISHOP often held and utilized a cellular telephone while committing the bank fraud.

4. On January 22, 2023, the Wheat Ridge Police Department (WRPD) in Colorado arrested BISHOP for an outstanding warrant out of Montgomery County, Texas. A WRPD officer had stopped BISHOP for jaywalking in Wheat Ridge, Colorado and a routine name check revealed that he had an outstanding warrant for Fraud Use/Possession of Identifying Information (MCSO). During a search incident to arrest, the WRPD officer discovered a counterfeit document which contained BISHOP's photograph and the name Michael Stivale. BISHOP also had a cellular telephone on his person. The WRPD officer took custody of BISHOP and his property and transferred him to the Jefferson County Jail in Colorado. On or about February 9, 2023, BISHOP was transferred to the Montgomery County Jail in Texas. I contacted the MCSO to verify whether BISHOP had a cellular telephone in his property. MCSO confirmed that BISHOP had a Samsung

BISHOP had a cellular telephone in his property. MCSO confirmed that BISHOP had a Samsung cellular telephone, IMEI: 357299882022186, and on March 23, 2023, HSI Houston, Texas took custody of the DEVICE as it may contain evidence of crimes (victim/s' information and/or details of fraudulent activities).

5. On March 29, 2023, BISHOP was indicted by a federal grand jury in the Southern District of Texas for violations of Title 18 U.S.C. § 1344, Bank Fraud and Title 18 U.S.C. § 1028A, Aggravated Identity Theft.

6. Based on my training and experience, as well as the other sources of information, I am aware of the following:

a. That criminal organizations utilize cellular telephones to communicate information related to criminal activity, particularly during the period immediately before, during or after a transaction involving fraud or other illicit activities;

b. That criminals often store telephone numbers, names of criminal associates, photos, text messages, and other types of communication messages within their cellular telephones;

c. That this stored information often contains information on current and past criminal associates, and may be used to identify co-conspirators who have not been identified or located;

d. That criminals often utilize electronic devices, including cellular telephones, to steal and/or store victims' information and to manufacture counterfeit documents;

e. And finally, that this stored electronic information can be used to determine the identity of individuals who had telephone contact with the target cellular

telephone/s immediately prior to the seizure of the telephone in the form of stored data identifying recent incoming and outgoing calls.

7. The DEVICE is currently in the lawful possession of the Homeland Security Investigations. It came into the HSI's possession on March 23, 2023, when HSI Houston, Texas, took custody of the DEVICE following BISHOP's arrest. The DEVICE was held as evidence and will be forensically analyzed.

8. The DEVICE is currently in storage at 25700 I-45 North Suite 200, Houston, Texas. In my training and experience, I know that the DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the DEVICE first came into the possession of HSI SAs.

TECHNICAL TERMS

9. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and

moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four

satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. Storage Medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media. Log Files are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote

location; and file transfer logs list detailed information concerning files that are remotely transferred.

g. Uniform Resource Locator (URL) is a reference (or address) to a resource on the Internet. A URL has two main components: the protocol identifier and resource name. For the URL http://google.com, the protocol identifier is http, and the resource name is google.com. The resource name is the complete address to the resource, and for many protocols the resource name contains a host name, file name, port number, and reference. If the URL is an active web link, it is normally underlined and/or highlighted in blue.

10. Based on my training, experience, and research, I know that the device has capabilities that allow it to serve as a storage device which can maintain historical video footage. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence related to the above-mentioned violations.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

11. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

12. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

13. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

14. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

15. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the DEVICE described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Jacqueline Olivas
Homeland Security Investigations
Special Agent

Submitted by reliable electronic means, sworn to,
signature attested telephonically per Fed.R.Crim.P. 4.1,
and probable cause found on April 4, 2023.

SAM S. SHELDON, UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a black Samsung cellular telephone, IMEI: 357299882022186, hereinafter the "DEVICE," recovered from Kevin Daniel BISHOP at the time of his arrest on January 22, 2023. The DEVICE is currently located at 25700 I-45 North Suite 200, Houston, Texas.

This warrant authorizes the forensic examination of the DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the DEVICE described in Attachment A that relate to violations of Title 18 U.S.C. § 1344, Bank Fraud and Title 18 U.S.C. § 1028A, Aggravated Identity Theft, including but not limited to:

a. Phone contacts stored

b. Phone call history

c. Text Messages

d. Photographs

e. GPS data

f. Any and all data related to fraud

2. Evidence of user attribution showing who used or owned the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.